

## ABSTRACT OF THE DISCLOSURE

## “Host-based Systematic Attack Detection Tool”

[0057] A vulnerability checking tool for a host computer designed to examine security logs of attempted logins and revocations, to detect systematic attacks of a wide variety, and to generate a report file that can be examined for information concerning these types of events. Host computer files which contain data regarding attempted accesses and logins are used to create an event list based upon event criteria. The list is evaluated using a "floating period" time frame which advances by single event steps while no violation is detected within a particular floating period, and which advances by "jumps" when violations are detected in a time period so as to reduce the possibility of "over reporting" violations related to the same set of events.